REMARKS

Reconsideration of this application, as amended, is respectfully requested.

Claims 1-45 are pending in the application, with Claims 1, 2, 21, 22, 31, 39 and 42 being the independent claims.

The Examiner rejected Claims 1-45 under 35 U.S.C. §112, first paragraph. The Examiner rejected Claims 1-45 under 35 U.S.C. §103(a) as being unpatentable over *Applicants' Admitted Prior Art* (hereinafter, *AAPA*) in view of U.S. Publication No. 2005/0047598 to *Kruegel* and U.S. Publication No. 2005/0047600 to *Newkirk*.

Regarding the §112 rejection, the Examiner contends that the independent claims do not explicitly disclose whether the key is received in response to the request for a new key or independent of the key request triggered by a second predetermined key. Independent Claims 1, 2, 21, 22, 39 and 42 have been amended to more clearly recite the subject matter of the present invention. For example, Claim 1 has been amended to recite that the new traffic encryption key is transmitted to subscriber stations upon generation of the new traffic encryption key. Support for the amendments can be found on pages 26-27 of the Specification. Independent Claim 31 already recites that the new specific key and the new traffic encryption key are transmitted in accordance with a predetermined time from a start time of an active lifetime of the traffic encryption key.

The independent claims have also been amended to recite that expiration of the second predetermined time triggers a request for the new traffic encryption key from the subscriber station when the subscriber station fails to receive the new traffic encryption key. The base station transmits the new traffic encryption key to the subscriber station in response to the request. Accordingly, Applicants assert that the rejection under 35 U.S.C. §112 should be withdrawn.

Regarding the §103(a) rejection, the Examiner contends that each element of the claims is taught, suggested or rendered obvious by the combination of *AAPA*, *Kruegel* and *Newkirk*. More specifically, the Examiner contends that *AAPA* teaches or suggests each element of Claim 1 with the exception of multicasting or broadcasting rekey materials from a base station to a group of subscribers by keeping track of a key schedule/cryptographic period so as to allow the base station to automatically update keys for a group of subscriber stations. The Examiner cites *Kruegel* and *Newkirk* in an attempt to remedy these deficiencies.

The Examiner admits that *AAPA* does not disclose the newly added limitation, but contends that the limitation was not considered because it does not clarify the relationship between key request and key delivery based on the predetermined time and the second predetermined time. As described above, Claim 31 clearly describes that the new specific key and the new traffic encryption key are transmitted in accordance with the predetermined time, and no further clarification is required. Accordingly, the Examiner was required to examine the merits of each limitation of independent Claim 31 in the latest Office Action, and has failed to do so.

The Examiner has again failed to address the claims individually in the Office Action. Under MPEP § 707.07(d), "[a] plurality of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group." The Examiner has failed to explain how the rejection is equally applicable to all of the elements of Claims 1-45. Moreover, under 37 CFR § 1.104(c)(2), "The pertinence of each reference, if not apparent, must be clearly explained and *each rejected claim specified*." (emphasis added). For example, the Examiner fails to provide any support for the rejection of the dependent claims. Consequently, the rejections are improper.

Amended Claim 1 to recites that the predetermined time from the start time is managed by the base station and is less than a second predetermined time from the start time managed by the subscriber station. Expiration of the second predetermined time triggers a request for the new traffic encryption key at the subscriber station when the subscriber station fails to receive

the new traffic encryption key. The base station transmits the new traffic encryption key to the subscriber station in response to the request.

AAPA describes a system in which a subscriber station manages a TEK grace time in order to periodically update the TEK and thus receive a seamless and stable traffic service. *Kruegel* discloses a method for managing multiple cryptographic periods in a single cryptographic group. Specifically, *Kruegel* describes that a key management facility stores cryptographic periods of each storage location number. A system cryptographic period is created based on the storage location number cryptographic periods.

While *Kruegel* describes the management of a time period away from a subscriber station, it fails to disclose how a specific predetermined time managed away from the subscriber station relates to another time managed by the subscriber station. Specifically, *Kruegel* fails to disclose that a predetermined time from a start time of an active lifetime of a current traffic encryption key is managed by the base station, and that the predetermined time is less than a second predetermined time from the start time that is managed by the subscriber station, as recited in amended Claim 1. Further, *Kruegel* fails to disclose that the expiration of the second predetermined time triggers a request for the new traffic encryption key at the subscriber station when the subscriber station has failed to receive the new traffic encryption key, as recited in amended Claim 1. Thus, *Kruegel* fails to remedy the deficiencies of *AAPA*.

Newkirk describes the decryption of an encryption key, and also fails to remedy the deficiencies of *AAPA* described above. Therefore, amended Claim 1 is patentable over the combination of *AAPA*, *Kruegel* and *Newkirk*.

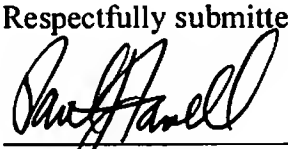
The Examiner also rejected independent Claims 2, 21, 22, 31, 39 and 42 under 35 U.S.C. §103(a). The Examiner has failed to address the claims individually in the Office Action. However Claims 2, 21, 22 and 31 have been amended in a manner similar to that of Claim 1. Further, the combination of *AAPA*, *Kruegel* and *Newkirk* fails to teach, suggest or render obvious operation methods of a traffic encryption key state machine, as recited in Claims 39 and 42. In

view of the above, Claims 2, 21, 22, 31, 39 and 42 are also patentable over the combination of *AAPA*, *Kruegel* and *Newkirk*.

Regarding Claims 3-20, 23-30, 32-38, 40, 41 and 43-45, while not conceding the patentability of the dependent claims, *per se*, Claims 3-20, 23-30, 32-38, 40, 41 and 43-45 are also patentable for at least the above reasons. Accordingly, Applicants assert that Claims 1-45 are allowable over *AAPA*, *Kruegel*, *Newkirk*, or any combination thereof, and the rejection under 35 U.S.C. §103(a) should be withdrawn.

Accordingly, all of the claims pending in the Application, namely, Claims 1-45 are believed to be in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicants' attorney at the number given below.

Respectfully submitted,



Paul J. Farrell
Registration No. 33,494
Attorney for Applicant(s)

THE FARRELL LAW FIRM, LLP
290 Broadhollow Rd., Ste. 210 E
Melville, New York 11747
(516) 228-3565